

# Unit 18 Homework: Lets go Splunking!

## Step 1: The Need for Speed

Answer the following questions:

- Based on the report created, what is the approximate date and time of the attack?
  - How long did it take your systems to recover?
- The attack began at 2020-02-23 at 2:30pm(14:30) and lasted until 2020-02-23 at 10:30pm(22:30)**

Submit a screen shot of your report and the answer to the questions above.

New Search

Save As Create Table View Close

source="server\_speedtest.csv" host="Speedtest2" sourcetype="csv" | eval ratio='UPLOAD\_MEGABITS'/'DOWNLOAD\_MEGABITS'| table \_time, IP\_ADDRESS, DOWNLOAD\_MEGABITS, UPLOAD\_MEGABITS, ratio

All time

23 events (before 3/3/21 5:01:07.000 AM) No Event Sampling

Job

Verbose Mode

Events (23) Patterns Statistics (23) Visualization

100 Per Page Format Preview

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	0.0497
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	0.0520
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	0.0609
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	0.0696
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	0.0781
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	0.0865
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	0.09628
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	0.1087
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	0.1170
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	0.1252
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	0.0690
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	0.0774
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	0.0871
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831

## Step 2: Are We Vulnerable?

- Create a report that shows the `count` of critical vulnerabilities from the customer database server.
  - The database server IP is `10.11.36.23`.
  - The field that identifies the level of vulnerabilities is `severity`.
- Build an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, have an alert emailed to `soc@vandalay.com`.

Submit a screenshot of your report and a screenshot of proof that the alert has been created.

**Critical Vulnerability Cou...** Save Save As View Create Table View Close

source="nessus\_logs.csv" host="Nessus\_log" sourcetype="csv" dest\_ip="10.11.36.23" severity=critical | stats count as critical All time

✓ 49 events (before 3/3/21 5:41:17.000 AM) No Event Sampling Job || ↻ ⏏ ⬇ ⚙ Verbose Mode

Events (49) Patterns **Statistics (1)** Visualization

100 Per Page Format Preview

critical

49

▼ Critical Vulnerability Count Alert Open in Search Edit admin search Private Enabled

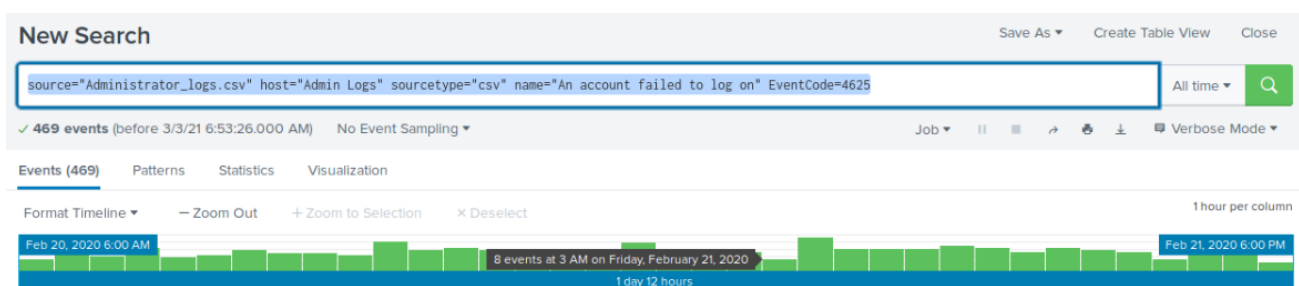
Enabled: ..... Yes. [Disable](#)  
 Permissions: ..... Private. Owned by admin. [Edit](#)  
 Modified: ..... Mar 3, 2021 5:50:13 AM  
 Alert Type: ..... Scheduled. Daily, at 0:00. [Edit](#)  
 Trigger Condition: .. Number of Results is = 1. [Edit](#)  
 Actions: ..... 1 Action [Edit](#)  
 ☐ Send email

## Step 3: Drawing the (base)line

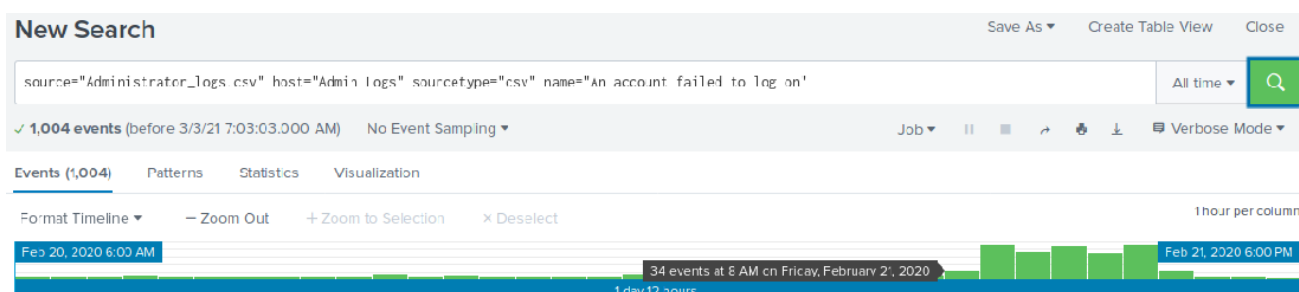
1. When did the brute force attack occur?  
**2021-02-21**
2. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.
3. Design an alert to check the threshold every hour and email the SOC team at [SOC@vandalay.com](mailto:SOC@vandalay.com) if triggered.

Submit the answers to the questions about the brute force timing, baseline and threshold. Additionally, provide a screenshot as proof that the alert has been created.

**Using:** source="Administrator\_logs.csv" host="Admin Logs" sourcetype="csv" name="An account failed to log on" EventCode=4625 **Based on the Visual Representation 8 would be a suited amount for a triggered email alert.**



**Using :** source="Administrator\_logs.csv" host="Admin Logs" sourcetype="csv" name="An account failed to log on" **Based on the Visual Representation 15 would be a suited amount for a triggered email alert.**



### Potential Hourly Alert

Failed Log-Ins

Open in Search

Edit

admin

search

Private

Enabled

The number of failed logins is higher than usual. This may be a Brute Force Attack

Enabled: ..... Yes. [Disable](#)

Permissions: ..... Private. Owned by admin. [Edit](#)

Modified: ..... Mar 3, 2021 6:33:35 AM

Alert Type: ..... Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 15. [Edit](#)

Actions: ..... [1 Action](#)

[Send email](#)